Kiley L. Grombacher (State Bar No. 245960)
BRADLEY/GROMBACHER LLP
31365 Oak Crest Drive, Suite 240
Westlake Village, CA 91361
Telephone: 805-270-7100
Email: kgrombacher@bradleygrombacher.com

Attorney for Plaintiffs

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

SACRAMENTO DIVISION

JACLYN BROOKE FAIRCLOTH as guardian ad litem of H.F.; and on behalf of all others similarly situated,

Plaintiff,

vs.

POWERSCHOOL GROUP LLC and POWERSCHOOL HOLDINGS, INC.

Defendants.

CLASS ACTION COMPLAINT FOR DAMAGES, INJUNCTIVE RELIEF, AND EQUITABLE RELIEF FOR:

1. Invasion of Privacy;
2. Breach of Implied Contract;
3. Unjust Enrichment;
4. Negligence
5. Negligence Per Se
6. Breach of Third-Party Beneficiary Contract

JURY TRIAL DEMANDED

Jaclyn Brooke Faircloth as guardian ad litem of H.F. ("Plaintiff" or "H.F."), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants PowerSchool Group LLC and PowerSchool Holdings, Inc. ("Defendants") and alleges, upon personal knowledge as to Plaintiff's own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This class action lawsuit arises out of Defendants' failure to implement reasonable and industry standard data security practices to properly secure, safeguard, and adequately destroy Plaintiff's and the proposed Class Members' personally identifiable information ("PII") and personal health information ("PHI") (collectively, "Sensitive Information") that it acquired and stored as part of its business relationship with school systems throughout the United States and North America.

2. Defendant collected and maintained certain PHI and PII of Plaintiff and the proposed Class Members (defined below), who are (or were) students and faculty of schools that used Defendant's PowerSchool platform.

3. Plaintiff and the proposed Class Members trusted Defendant to maintain and secure their Sensitive Information on the understanding that Defendant would protect it against disclosure.

4. Instead, Plaintiff's and Class Members' Sensitive Information was targeted, compromised, and unlawfully accessed due to Defendants' lax security measures on December 28, 2024, when cybercriminals compromised Defendant's information systems, which contained Plaintiff's and other individuals Sensitive Information. (hereinafter, the "Data Breach")

5. The Sensitive Information compromised in the Data Breach was exfiltrated by cybercriminals who target such Sensitive Information for its value to

identity thieves.

6. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect consumers' Sensitive Information, which it was hired and expected to protect, from a foreseeable and preventable cyber-attack.

FACTUAL ALLEGATIONS

The Data Breach

7. On December 28, 2024, PowerSchool, an education technology platform for K-12 education housing the data of over 60 million students and more than 18,000 customers—namely school systems—worldwide, was infiltrated by cybercriminals who accessed highly Sensitive Information of students and educators.

8. The cybercriminals gained access to PowerSchool's Student Information System (SIS) database through its customer support portal using compromised credentials due to PowerSchool's lack of robust authentication and access control security measures. The cybercriminals then used maintenance access channels to access data stored on the school district's PowerSchool servers.

9. The Data Breach exposed highly sensitive, personal information, of students and educators, including but not limited to names, addresses, contact information, Social Security numbers, medical data, and grades dating back to 2005. This unauthorized access is particularly concerning given the high value of pediatric protected PHI to cybercriminals.

10. Despite the severity of the breach, PowerSchool has not notified the families of affected students or educators whose Sensitive Information was compromised. Rather, it has primarily communicated with its clients (school systems), leaving many families potentially unaware of the risks to their children's Sensitive information.

11. Defendants' failure to timely detect and notify the end-users of its product of the Data Breach made its end users vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

12. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of misuse of their Sensitive Information.

13. Defendants maintained and used the Sensitive Information in a reckless manner. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Sensitive Information was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition. In addition, Defendant failed to properly maintain and monitor the computer network and systems that housed the Sensitive Information.

14. Moreover, if Defendants had implemented reasonable logging, monitoring, and alerting systems, it would have known about the malicious activity

soon enough to enable it to stop the attack.

15. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to take standard and reasonably available steps to prevent the Data Breach; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Sensitive Information; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

16. Plaintiff's and Class Members' PII, finances, and identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained has been accessed and acquired by data thieves.

17. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiff's and Class Members' Sensitive Information was targeted, accessed, and been misused, and because the data stolen includes all the necessary ingredients to allow cybercriminals to perpetrate financial and identity fraud.

18. Because of the Data Brach, Plaintiff and the Class Members face a current, imminent, and ongoing risk of fraud and identify theft

19. At all relevant times, Defendants knew it was storing Plaintiff's and Class Members' Sensitive Information, and that, as a result, Defendant's systems

would be attractive targets for cybercriminals.

20. Defendants also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Sensitive Information was compromised, especially given that Data Breaches have become unfortunately ubiquitous.

21. PII and PHI have considerable value and constitute an enticing and well-known target to hackers. Hackers easily can sell stolen data because of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[1]

22. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the ITRC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non- sensitive" records.[2]

23. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as

---

[1] Brian Krebs, The Value of a Hacked Company, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited June 29, 2024).
[2] Data Breach Reports: 2019 End of Year Report, IDENTITY THEFT RESOURCE CENTER, at 2, available at https://notified.idtheftcenter.org/s/resource#annualReportSection.

many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[3]

24. Even if stolen Sensitive Information does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

25. Defendant agreed to and undertook legal duties to maintain the protected personal information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Under state and federal law, businesses like Defendants' have a duty to protect their clients' current and former customers' Sensitive Information and to notify them about breaches.

26. Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff

[3] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1).

and Class Members must immediately devote time, energy, and money to: closely monitor their bank statements, bills, records, and credit and financial accounts; change login and password information on any sensitive account even more frequently than they already do, more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack, and search for suitable identity theft protection and credit monitoring services, and pay to procure them

27. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' customers especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

28. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[4]

29. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendants fails to undertake the necessary and appropriate security and training

[4] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

measures to protect Plaintiff's and Class Members' Sensitive Information.

30. Because of Defendant's ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

31. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

32. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

33. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

34. Cybercriminals need not harvest a person's Social Security number or financial account information to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and Class Members' financial accounts.

35. Upon information and belief, Defendant has committed to offering credit monitoring services to victims, which does not adequately address the lifelong harm that Plaintiff and Class Members will face.

36. The risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information significant and will persist for years.

37. Upon information and belief, Defendant failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing Sensitive Information.

Defendants

38. Defendants together operate PowerSchool, an education technology platform for K-12 education, which serves over 60 million students and more than 18,000 customers worldwide.

39. As part of its business, Defendant receives and maintains the Sensitive

Information of thousands of consumers, including students and educators.

40. In collecting and maintaining Sensitive Information, Defendant implicitly agreed it would safeguard the data in accordance with its internal policies, state law, and federal law.

41. Defendant understood the need to protect consumers' Sensitive Information and prioritize its data security.

42. Indeed, Defendant's Privacy policy acknowledges that "We seek to protect our customers' personal data from unauthorized access, use, modification, disclosure, loss, or theft by leveraging various reasonable security measures and methods[.]"[5]

43. Despite acknowledging a duty to do so, Defendant failed to implement reasonable cybersecurity safeguards or policies to protect Plaintiff's and Class Members' Sensitive Information.

44. As a result, Defendant's security faced significant vulnerabilities that allowed cybercriminals to exploit and gain access to Plaintiff's and Class Members' Sensitive Information.

Plaintiff and the Proposed Class

45. H.F.is a nine-year-old who attends third grade at Brevard Elementary School in Brevard, North Carolina.

[5] PowerSchool, Privacy Policy, https://www.powerschool.com/privacy/ (last visited January 12, 2025).

46. Plaintiff's school uses Defendant's PowerSchool platform.

47. Upon information and belief, Plaintiff's Sensitive Information was compromised in the Data Breach.

48. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach, which includes time spent monitoring his information to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

49. Plaintiff is concerned for H.F.'s personal financial security and uncertainty over what Sensitive Information exposed in the Data Breach.

50. H.F. and Plaintiff suffered an actual injury from the exposure of his Sensitive Information, which has violated his rights to privacy.

51. Plaintiff has suffered an actual injury in the form of damages to and diminution in the value of his Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

52. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his Sensitive Information, which is now in the hands of unauthorized third parties and cyber criminals.

53. Defendant's offer of free credit monitoring does little to Protect H.F., as he has little to no established credit record at this time. However, hackers may still

use his information to take out credit cards and loans.

54. The risk to H.F.is great because his information can be used to create a "clean identity slate."

55. Plaintiff remains at a present and continued risk of harm due to the exposure and potential misuse of her personal data by criminal hackers.

56. Plaintiff has a continuing interest in ensuring that his Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

57. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and Class Members trusted Defendant with their Sensitive Information. But Defendant betrayed that trust by failing to employ proper data security practices prevent the Data Breach.

58. As a result of Defendant's unreasonable and inadequate data security practices, Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages, including but not limited to (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (g) deprivation of value of their PII; and (h) the continued risk to their Sensitive Information, which remains in the

possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it collected and maintained.

59. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

60. Plaintiff and Class Members may also incur out of pocket costs, e.g., for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

61. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

62. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated

63. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as

long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

Defendants Failed to Adhere to FTC Guidelines.

64. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

65. In 2016, the FTC updated its publication, Protecting Sensitive Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

66. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

67. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer, or in this case, consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Violated HIPPA.

70. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep consumers' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification

Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[6]

71. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[7]

72. The Data Breach itself resulted from a combination of inadequacies indicating Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. 17§ 164.312(a)(1);

---

[6] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth,
Social Security numbers, and medical record numbers.

[7] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

PARTIES

73. H.F. is nine years old and is a citizen of the state of North Carolina. At all relevant times, Plaintiff has been a resident of Brevard, North Carolina.

74. During the Class Period, Defendants collected Plaintiff's Sensitive Information.

75. Defendant, PowerSchool Group LLC, is a company incorporated in Delaware, with its principal place of business located at 150 Parkshore Drive Folsom, CA.

76. Defendant, PowerSchool Holdings Inc., is a company incorporated in Delaware, with its principal place of business located at 150 Parkshore Drive Folsom, CA.

JURISDICTION AND VENUE

77. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C.§1332(d)(2), because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from each Defendants

78. Defendants are each subject to personal jurisdiction in this district because they have substantial aggregate contacts throughout the United States and the state of California. Defendants have engaged, and continue to engage, in conduct that has a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, and the state of California, and this District, and it purposely availed itself of the laws of the United States and the State of California.

79. Defendants are each subject to personal jurisdiction in this District because they purposely avail themselves of the privilege of conducting activities in the United States and the State of California and direct business activities toward consumers throughout the United States and the State of California. Furthermore, Defendants engaged and continue to engage in conduct that has a foreseeable, substantial effect throughout the United States, the State of California, and this District connected with its unlawful acts. Defendants operate as a common

enterprise with principal places of business in California.

80. Venue is proper in this District under 28 U.S.C §1391(b) because Plaintiff and thousands of potential Class Members reside in this District; Defendants transact business in this District; and Defendants intentionally avails itself of the laws within this District.

CLASS ALLEGATIONS

81. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

82. The Classes that Plaintiff seeks to represent are defined as follows:

Nationwide Class

All individuals who reside within the United States whose Sensitive Information was accessed without authorization in the Data Breach (the "Class").

North Carolina Subclass

All residents of North Carolina whose Sensitive Information was accessed without authorization in the Data Breach (the "Class").

83. Collectively, the Class and North Carolina Subclass are referred to as the "Classes" or "Class Members."

84. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct

protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

85. Plaintiff reserves the right to amend the definitions of the Classes or add a Class or Subclass if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

86. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant, upon information and belief, millions of minor individuals are implicated.

87. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. The questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, includes the following:

a. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant was negligent in maintaining, protecting, and securing Sensitive Information;

d. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;

e. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. Whether Defendant's Email Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiff's and the Class's injuries;

h. What the proper damages measure is; and

i. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

88. Typicality: Plaintiff's claims are typical of those of the other members of the Classes because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

89. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendants' security policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

90. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no

relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

91. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

92. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since Defendants would be able to exploit and overwhelm the limited resources of each individual Class

Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

93. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

94. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

95. Unless a Class-wide injunction is issued, Defendants may continue to act unlawfully as set forth in this Complaint.

96. Further, Defendants have acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

CAUSES OF ACTION

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Classes Members v. All Defendants)

97. Plaintiff re-alleges and incorporates by reference all the allegations

contained in the foregoing paragraphs as if fully set forth herein.

98. As minor children, Plaintiff's minor child and Class Members had a legitimate expectation of privacy in their personally identifying information. Plaintiff and Class Members were entitled to the protection of this information from disclosure to unauthorized third parties.

99. Defendants owed a duty to Plaintiff and Class Members to keep their PII confidential.

100. Defendants permitted the public disclosure of Plaintiff's minor child's and Class Members' PII to unauthorized third parties.

101. The PII that was collected and disclosed without the Plaintiff's and Class Members' authorization was highly sensitive, private, and confidential. The public disclosure of the type of PII at issue here would be highly offensive to a reasonable person of ordinary sensibilities.

102. By permitting the unauthorized collection and disclosure, Defendants acted with reckless disregard for the Plaintiff's and Class Members' privacy, and with knowledge that such disclosure would be highly offensive to a reasonable person. Furthermore, the disclosure of the PII at issue was not newsworthy or of any service to the public interest.

103. Defendants acted with such reckless disregard as to the safety of Plaintiff's and Class Members' PII to rise to the level of intentionally allowing the intrusion upon the seclusion, private affairs, or concerns of Plaintiff and Class

Members.

104. Plaintiff and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes Members v. All Defendants)

105. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

106. Plaintiff and Class Members were required provide their Sensitive Information to Defendants as a part of obtaining an education. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for Defendants' products and/or services.

107. Defendants solicited, offered, and invited Class Members to provide their Sensitive Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their PII to Defendant.

108. Defendants accepted possession of Plaintiff's and Class Members' PII for the purpose of providing services to Plaintiff and Class Members.

109. Plaintiff and the Class Members entrusted their Sensitive Information to Defendant. In so doing, Plaintiff and the Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and

accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

110. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

111. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide Sensitive Information, was the latter's obligation to: (a) use such Sensitive Information for business purposes only, (b) take reasonable steps to safeguard that Sensitive Information, (c) prevent unauthorized disclosures of the Sensitive Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information, (e) reasonably safeguard and protect the Sensitive Information of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the Sensitive Information only under conditions that kept such information secure and confidential.

112. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendants on the other, is demonstrated by their conduct and course of dealing.

113. Upon information and belief, at all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby it

expressly that it would only disclose Plaintiff's and Class Members' Sensitive Information under certain circumstances, none of which relate to the Data Breach.

114. Upon information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Sensitive Information would remain protected.

115. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

116. Plaintiff and Class Members would not have entrusted their Sensitive Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

117. Plaintiff and Class Members would not have entrusted their Sensitive Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

118. Every contract has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

119. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

120. Defendant breached the implied contracts it made with Plaintiff and the

Class by failing to safeguard and protect their Sensitive Information, by failing to delete the Sensitive Information of Plaintiff and the Class once the relationship ended, and by failing to provide adequate notice to hem that Sensitive Information was compromised as a result of the Data Breach.

121. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Sensitive Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of Sensitive Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

122. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: invasion of privacy; theft of their Sensitive Information; uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; loss of benefit of the bargain; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; nominal damages; and the continued and certainly increased risk to their Sensitive Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as

Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information.

123. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

124. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Classes v. All Defendants)

125. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

126. Plaintiff brings this Count in the alternative to the breach of implied contract claim.

127. Plaintiffs and Class Members conferred a monetary benefit on Defendant when Defendant's clients provided Plaintiff's and Class Members' Sensitive Information to Defendant, which Defendant collected.

128. By obtaining Plaintiff's and Class Members' Sensitive Information, Defendants received a monetary benefit. Defendants knew that it could use Plaintiff's and Class Members' Sensitive Information for financial gain and has

retained that benefit.

129. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Sensitive Information.

130. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and the Class, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

131. Defendants have unjustly received and retained monetary benefits from Plaintiff's and Class Members by profiting off the use of their Sensitive Information under unjust circumstances such that inequity has resulted.

132. Defendants have knowingly obtained benefits from Plaintiff and Class Members as alleged herein under circumstances such that it would be inequitable and unjust for Defendants to retain them.

133. Plaintiff and Class Members are therefore entitled to relief, including disgorgement of all revenues and profits that Defendants earned as a result of its unlawful and wrongful conduct.

COUNT IV
Negligence
(On behalf of Plaintiff and the Classes v. All Defendants)

134. Plaintiff re-alleges and incorporates by reference all the allegations

contained in the foregoing paragraphs as if fully set forth herein.

135. Defendants required that Plaintiff and Class Members submit non-public Sensitive Information in the ordinary course of providing its products and/or services.

136. Defendants gathered and stored the Sensitive Information of Plaintiff and Class Members as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

137. Plaintiff and Class Members entrusted Defendant with their Sensitive Information with the understanding that Defendant would safeguard their information.

138. Defendant had full knowledge of the sensitivity of the Sensitive Information and the types of harm that Plaintiff and Class Members could and would suffer if the Sensitive Information were wrongfully disclosed.

139. By voluntarily undertaking and assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Plaintiff's Class Members' Sensitive Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data

breach.

140. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

141. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks adequately protected the Sensitive Information.

142. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their Sensitive Information, a necessary part of being attaining an education.

143. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Sensitive Information.

144. Defendants were subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

145. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former students' and educators' Sensitive Information it was no longer required to retain pursuant to regulations.

146. Moreover, Defendants had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

147. Defendants had and continues to have a duty to adequately disclose that the Sensitive Information of Plaintiff and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Sensitive Information by third parties.

148. Defendants breached their duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Sensitive Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Sensitive Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' Sensitive Information;

d. Failing to detect in a timely manner that Class Members' Sensitive Information had been compromised;

e. Failing to remove former customers' Sensitive Information it was no

longer required to retain pursuant to regulations, and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

149. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

150. Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

151. Plaintiff and Class Members were within the class of persons the FTC Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statute was intended to guard against.

152. Defendants' violation of Section 5 of the FTC Act constitutes negligence. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

153. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

154. It was foreseeable that Defendants' failure to use reasonable measures

to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

155. Defendants have full knowledge of the sensitivity of the Sensitive Information and the types of harm that Plaintiff and the Class could and would suffer if the Sensitive Information were wrongfully disclosed.

156. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Sensitive Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Sensitive Information, and the necessity for encrypting Sensitive Information stored on Defendant's systems or transmitted through third party systems.

157. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Sensitive Information would result in one or more types of injuries to Class Members.

158. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

159. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

160. Defendants' duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in

situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard Sensitive Information.

161. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Sensitive Information of Plaintiffs and the Class would not have been compromised.

162. There is a close causal connection between Defendants' failure to implement security measures to protect the Sensitive Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Sensitive Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Sensitive Information by adopting, implementing, and maintaining appropriate security measures.

163. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: invasion of privacy; theft of their Sensitive Information; uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; loss of benefit of the bargain; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; statutory

damages; nominal damages; and the continued and certainly increased risk to their Sensitive Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Sensitive Information.

164. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

165. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

166. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT V
Negligence Per Se
(On behalf of Plaintiff and the Classes v. All Defendants)

167. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

168. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Sensitive Information.

169. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, consumers' Sensitive Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's Sensitive Information.

170. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which did occur.

171. Defendants breached their duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Sensitive Information.

172. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its consumers, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law.

173. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a Data Breach.

174. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l).

175. Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

176. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Sensitive

Information.

177. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

178. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

179. The harm resulting from the Data Breach was the harm the FTC Act was intended to guard against, and Plaintiff and Class Members are within the class of persons the statute was intended to protect.

180. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that it was failing to meet its duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Sensitive Information.

181. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: invasion of privacy; theft of their Sensitive Information; uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; loss of benefit of the bargain; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; statutory damages; nominal damages; and the continued and certainly increased risk to their

Sensitive Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Sensitive Information.

182. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT VI
Breach of Third-Party Beneficiary Contract
(On behalf of Plaintiff and the Classes v. All Defendants)

183. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

184. Defendant entered contracts with its clients to provide services that explicitly or implicitly included data security practices, procedures, and protocols sufficient to safeguard the Sensitive Information that was to be entrusted to it.

185. Indeed, because such safeguards are required by industry standard and applicable statutory, common, and regulatory law, the implementation and maintenance of such safeguards is required to fulfill a parties' contractual obligations of good faith and fair dealing in their performance.

186. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their Sensitive Information that Defendant agreed to receive and

protect through its services. Thus, the benefit of collection and protection of the Sensitive Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties, and Plaintiff and Class Members were direct and express beneficiaries of such contracts. Indeed, the sole purpose of the contracts was to enable the provision of education services to Plaintiff and the proposed Class Members.

187. Defendants knew that if it were to breach these contracts with its clients, Plaintiff and Class Members would be harmed.

188. Defendants breached its contracts with its clients and, as a result, Plaintiff and Class Members were affected by this Data Breach when Defendants failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

189. As foreseen, Plaintiff and the proposed Class Members were harmed by Defendants' failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their Sensitive Information and the loss of control over how it was used and who had access to it.

190. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection,

and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of the services they paid for and received.

191. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes alleged herein, respectfully requests that the Court enter judgment as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as the representatives for the Classes and counsel for Plaintiff as Class Counsel;

B. For an order declaring the Defendants' conduct violates the statues and causes of action referenced herein;

C. For an order finding in favor of Plaintiff and Class Members on all counts asserted herein;

D. Ordering Defendants to pay for lifetime credit monitoring and dark web scanning services for Plaintiff and the Classes;

E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

F. For prejudgment interest on all amounts awarded;

G. For an order of restitution and all other forms of equitable monetary relief requiring the disgorgement of the revenues wrongfully retained as a result of the Defendants' conduct;

H. For injunctive relief as pleaded or as the Court may deem proper; including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the Sensitive Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Sensitive Information for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Sensitive Information of Plaintiff and Class Members;

vi. prohibiting Defendants from maintaining the Sensitive Information of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendants to segment data by, among other things, creating firewalls and controls so that if one area of Defendants' network is compromised, hackers cannot gain access to portions of Defendants' systems;

xi. requiring Defendants to conduct regular database scanning and security checks;

xii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the Sensitive Information of Plaintiff and Class Members;

xiii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting p Sensitive Information;

xv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xviii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

I. For an order awarding Plaintiff and Class Members their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and

J. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demand a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

DATED: January 17, 2025

Respectfully submitted by:

By: /s/ *Kiley L. Grombacher*
Kiley L. Grombacher, Esq.
Attorneys for Plaintiff